Shift – 소개 백서

Phantom: 분산형 스토리지 제품군

버전 1.1.0

Isabella Dell - Craig Campbell - Ralf S.

2018년 5월 10일

목차

요약

정보의 검열과 억제는 인류 역사에서 흔한 문제였습니다. 블록 체인 및 기타 분산형 기술의 도래로 콘텐츠를 쉽게 검열할 수 없도록 하는 기술 혁명을 가져왔습니다. 스토리지와 표시 계층 기술이 결합되어 검열로부터 데이터를 보호할 수 있는 기능과 함께 최종 사용자 및 운영자의 역량을 강화할 수 있게 되었습니다.

Shift는 검열 문제에 대한 해법을 제시하고 이러한 새로운 기술의 결합을 통해 주어진 문제를 어떻게 해결할지를 정의합니다.

1 소개

이 백서는 분산형 시스템에서 콘텐츠 호스팅 플랫폼으로 사용되는 통합 기술 제품군인 Phantom을 소개합니다. 이 문서의 범위는 Shift에서 채택하고 있는 일반적인 기술 접근 방식에 대해 구체적으로 설명하는 것입니다. 본 백서에서는 Shift가 Phantom을 통해 해결하고자 하는 문제를 정의하고 다양한 기술을 활용하여 문제를 어떻게 다룰지를 기술하고 있습니다.

1.1 문제 정의

오늘날의 세상에서는 인터넷 사업자가 정보 자유에 대한 가장 큰 잠재적 위협 요소입니다. 서버 호스트, 정부 및 ISP(인터넷 서비스 공급자)는 웹을 통제하며, 서버 운영 중지, 블랙리스트 작성 및 DNS(도메인 이름 시스템) 인수를 통해 콘텐츠에 대한 액세스를 제거할 수 있습니다. 현재 사용 가능한 인터넷 기술은 당국과 인터넷에 대한 당국의 공격을 막을 만큼 충분히 성숙되지는 않았습니다. 검열 위협을 완화하기 위해 새로운 분산형 인터넷을 구축하는 데 활용될 IPFS(InterPlanetary File System) (Benet, 2014) 및 기타 기술이 대기 상태에 있습니다.

1.2 문제 분석

1.2.1 망 중립성 및 인터넷 서비스 공급자

ISP는 오늘날 거의 모든 최종 사용자에게 인터넷의 단일 진입점의 역할을 합니다. 이들 기관은 일반적으로 고객에게 연결성을 제공하는 사설 상용 엔터티입니다. ISP는 쉽게 사라지지는 않을 것입니다. 현재 ISP가 인터넷 자유를 위협하는 것은 분명합니다. 2000년대 후반에는 ISP가 최종 사용자 활동을 조작했던 사례가 있었습니다. Comcast는 BitTorrent 사용자를 대상으로 하는 트래픽 성형(traffic shaping) 형태를 구현하여 (to Marlene H. Dortch, 2008; Eckersley, 2007), 이들이 자유롭게 사용 가능한 콘텐츠라 할지라도 액세스하기로 선택한 콘텐츠에 액세스할 수 없도록 했습니다. 유료 고객에 대한 이 공격은 망 중립성 원칙, 즉 출처와 관계 없이 모든 콘텐츠와 애플리케이션에 액세스할 수 있어야 한다는 원칙에 대한 위반으로 간주되어야 합니다.

망 중립성은 인터넷의 시작 이후 인터넷을 통제했던 불문의 개념이었습니다. 정보의 자유는 모든 인류에 유익하도록 기술을 발전시키기 위한 기본 요건으로 여겨져 왔습니다. 망 중립성에 대한 잠재적 위협 중 하나는 자신들이 동의하지 않는 콘텐츠에 대한 액세스를 차단, 제한 또는 저속화할 수 있는 ISP에서 비롯됩니다. ISP는 콘텐츠에 대한 프리미엄 액세스에 대해 더 비싼 요금을 부과하려 할 수도 있습니다. ISP를 우회하기는 일반적으로 불가능하지만, 콘텐츠 공급자는 새로운 기술을 이용하여 콘텐츠를 분산시키고 ISP가 쉽게 검열할 수 없는 방식으로 콘텐츠를 확산할 수 있습니다.

1.2.2 정부 기관

범정부 차원에서 법률 집행, 테러 방지 및 첩보 수집 활동과 관련하여 인터넷과 이해 관계를 맺고 있습니다. 이러한 권능과 책임을 감안하여 정부는 또한 사법 제도를 통해 인터넷에 대한 여러 권한이 부여되기도 합니다. 예컨대, 미국에서는 FBI가 적절한 영장이 발부된 경우 웹사이트나 서비스를 중지시킴으로써(Search.usa.gov, 2018), 사실상 웹사이트를 검열하는 효과를 발휘할 수 있습니다. 경우에 따라, FBI는 더 많은 증거를 확보할 목적으 더 광범위한 네트워크를 캐스팅하여 웹 사이트의 용도를 변경하기도 합니다. 이러한 스타일의 인수는 일반적으로 심각한 범죄 활동(Silk Road, 불법 서비스)에서 사용되지만 개인의 자유에 대한 직접적인 공격을 나타냅니다. (Martin, 2013).

인터넷에 대한 정부 공격의 기타 예는 정치 분야에서 찾아 볼 수 있습니다. 2017년 9월에 스페인 정부는 ".cat"에 대한 최상위 도메인 공급자를 소유했으며, 따라서 해당 범위 내에서 실행되는 DNS에 대한 모든 권한이 사실상 이 기관(정부)에 부여되었습니다. 뿐만 아니라, 이 정부는 카탈로니아 국민투표를 지지하는 웹사이트를 강제로 검열하기 시작했으며 결국 투표소에서 투표를 제출하지 못하게 했습니다. 정부 검열은 오늘날 인터넷의 명백하고 현존하는 위험입니다. 새로운 인터넷은 이러한 과거의 문제에서 진화하여 정보를 자유롭게 이용 가능한 상태로 유지해야 합니다.

1.2.3 중앙집중식 서버 호스팅

Amazon이나 Microsoft 같은 서버 공급자 및 사업자는 웹사이트나 다른 애플리케이션을 호스팅할 수 있는 시스템을 제공합니다. 흔히 이들 공급자는 정부 기관과 정부 기관의 서비스 해지 요청에 대해 지나치게 협조적 태도를 보였습니다. (Raphael, 2009; Chen, 2017). 또한, 이들은 인터넷 환경에서 중앙집중식으로 운영됩니다. 2017년 초에 Amazon S3 East의 서비스 중단은 수십만 개의 웹사이트에 영향을 미쳤습니다 (Amazon, 2018). 이 서비스 중단 동안 여러 주요 웹사이트에 전혀 액세스할 수 없었으며 인터넷의 상당 부분이 가동되지 못했습니다.

인터넷이 계속 확장됨에 따라, 이들 공급자는 점점 더 많은 사용자로부터 호스팅 요구를 받기 때문에 이러한 문제도 점점 더 자주 발생할 수 있습니다. 이 문제는 IPFS 같은 최신 기술을 사용하여 완화할 수 있지만, 웹사이트를 IPFS로 전환하여 대중에게 제공하는 인프라는 광범위하게 활용되고 있지 않습니다.

1.3 솔루션 제안

웹 집중화 및 검열 문제를 해결하기 위해서는 단일 서비스 장애 지점을 제거하거나 완화할 수 있는 시스템이나 소프트웨어 계층이 있어야 합니다. 웹에는 서버 호스트, DNS(도메인 이름 서비스) 공급자 및 WAN(광역 네트워크)와의 인터넷 연결 같은 다양한 서비스 장애 지점이 있습니다. 안타깝게도, WAN 연결 문제 해결은 이 문서의 범위를 벗어나지만, 서버 호스팅 및 DNS 문제는 Shift에서 개발 중인 Phantom이라는 소프트웨어 제품군 사용으로 완화할 수 있습니다. Phantom은 분산화용으로 제작된 기술 스택을 제공하는 계층화된 애플리케이션입니다.

Phantom은 여러 웹 검열원에 대한 솔루션을 제공합니다. 이름에서 알 수 있듯이, Phantom에 호스팅되는 서비스는 한 호스트에서 사라지더라도 네트워크의 다른 호스트에서 계속 액세스할 수 있습니다. Phantom은 IPFS 백본을 구현하여 Shift 네트워크의 스토리지 계층을 생성합니다. 최종 사용자는 블록체인 기반 공간 임대 시스템을 사용하여 장기 보관을 위해 파일을 제출할 수 있습니다. 웹사이트 운영자는 Hydra를 사용하여 Shift 스토리지 클러스터에서 전체 웹사이트를 제공함으써 리소스를 렌더링하고 검열 중일 경우 검색용으로 리소스를 동적으로 업데이트하는 Jenga를 사용하여 콘텐츠를 실시간으로 유지할 수 있습니다. 이 기술 제품군은 쉽게 검열될 수 없는 완벽한 최종 사용자 환경을 구현합니다.

2 스토리지 계층

2.1 InterPlanetary 파일 시스템

Phantom 스토리지 계층은 InterPlanetary 파일 시스템이라 명명된 자유롭게 사용할 수 있는 기술로 구성됩니다. IPFS는 여러 분산된 스토리지 애플리케이션에 대한 백본으로 사용되는 피어 투 피어 하이퍼미디어 분산 프로토콜 (Benet, 2014)입니다. IPFS는 웹 애플리케이션 및 기타 타입의 콘텐츠를 제공하는 데 적합한 분산형 파일 시스템을 구현하기 위한 체계적으로 문서화된 프로토콜을 제공합니다. IPFS는 중앙의 서비스 장애 지점이 없는 완전한 피어-투-피어로, 모든 사용자가 시스템에 참여할 수 있습니다. 이 파일 시스템 프로토콜의 운영 관리는 중앙 기관에만 의존하지 않습니다. IPFS는 검열로부터 자유로운 새로운 분산형 인터넷 인프라를 구축할 준비를 갖추었습니다.

2.2 구현 – Shift 스토리지 클러스터

IPFS 인프라의 기본 상태는 전체 공유 네트워크로 제시됩니다. 이는 데이터 무결성, 가용성 및 맞춤 구현 문제(예: 스토리지 노드 실행을 위한 토큰 획득 보상)가 이어질 수 있습니다. 이러한 이유로 Shift는 사적 스왐(private swarm)을 실행합니다. 스토리지 노드에서 맞춤 스왐 키를 사용하여 동일 키를 사용하는 다른 노드하고만 대화할 수 있도록 합니다. 또한 사용 중인 Shift 노드가 Shift 네트워크 외부에 추가된 콘텐츠를 호스팅하고 서비스를 제공할 수 없도록 하여 안정성과 성능을 개선하고 있습니다.

IPFS는 데이터를 영구적으로 저장하기 위해 고정(pinning)이라는 개념을 구현합니다. 콘텐츠 고정은 콘텐츠를 영구적으로(즉 고정이 해제될 때가지) 사용할 수 있음을 의미합니다. 기본적으로 고정은 고정된 단일 피어에만 적용되며, 이는 시스템이 오프라인으로 전환될 경우 콘텐츠가 손실될 수 있음을 의미하기도 합니다. 이 문제는 Shift 피어만을 포함하는 IPFS 데몬을 실행하는 서브넷(또는 사적 네트워크)인 IPFS 클러스터를 사용하여 해결할 수 있습니다.

Shift 클러스터는 IPFS 데몬 주변에서 래퍼로서 가동됩니다. 최종 사용자는 IPFS 노드 그룹에 연결하여 그룹 내에 콘텐츠를 저장 및 복제할 수 있습니다. Shift 클러스터는 어느 위치에 어떤 콘텐츠를 사용할 수 있는지 추적하는 일을 담당할 리더를 선정합니다.

Shift 클러스터는 IPFS에 사용할 모듈식 클러스터링 시스템을 제공합니다. 이 클러스터링 시스템과 IPFS 데몬이 서로 연동하여 다음 작업을 수행합니다:

1. 피어에 콘텐츠 고정, 고정 해제 및 재고정
2. 통신용 HTTP API 제공
3. 클러스터 합의 주장 및 준수
4. 복제 팩터
5. 파일 저장 및 검색

이러한 기능이 결합하여 공용 IPFS 네트워크와는 완전히 독립적으로 동작하는 확장 가능한 분산형 스토리지 시스템을 제공합니다. 이는 사용자가 시스템 안에 콘텐츠를 삽입하고 유지할 때 반드시 필요합니다.

2.2.1 파일 고정

IPFS를 운영하는 동안 일정 시간이 경과한 이후 사용하지 않은 파일은 자동으로 삭제됩니다. 파일을 영구적으로 유지하려면 시스템 안에 고정해야 합니다. 파일을 고정하면 가비지 수집 프로세스에서 항목을 영구적으로 제거할 수 없으므로 항목을 항상 클러스터 내에서 사용할 수 있게 됩니다.

2.2.2 HTTP API

IPFS는 네트워크와 상호 작용하는 데 필요한 내부 명령 및 함수 모음을 제공합니다. 이와 동일한 함수 세트가 HTTP API로 미러링되므로 외부 소프트웨어가 시스템과 상호작용할 수 있습니다. 이러한 기능을 활용하여 Phantom은 최종 사용자가 클러스터에 합류하지 않아도 IPFS와 원격으로 통신할 수 있게 합니다.

2.2.3 합의

IPFS 클러스터에 저장된 모든 정보를 동기화 상태로 유지하려면 노드들 사이의 합의가 요구됩니다. 합의는 무기한 저장되어야 하는 고정된 콘텐츠의 경우 특히 중요합니다. 오프라인으로 전환되거나 새 리더가 선정될 때까지 하나의 노드가 리더로 선정되어 작동합니다.

2.2.4 복제 팩터

Shift에서 호스팅된 클러스터는 현재 각 콘텐츠 부분을 중복 노드로 복제하여 데이터가 손실되는 것을 방지하도록 구성되어 있습니다. 다시 말해서 각 파일이 기본 위치 이외의 여러 추가 위치에 백업된다는 뜻입니다. 백업 위치 중 하나를 사용할 수 없게 되는 경우, 클러스터는 콘텐츠를 추가 노드로 자동 복제합니다. 따라서 데이터를 모든 노드로 복사하지 않아도 되므로 네트워크를 확장할 수 있습니다.

2.2.5 파일 저장 및 검색

데이터가 시스템 내에서 고정되었으며 참여 노드가 전달된 데이터를 수신하고 나면, 스토리지 노드는 클러스터에 해당 데이터를 보관합니다. 해당 데이터의 요청이 서비스 노드에서 스토리지 노드에 도착하면 스토리지 노드는 데이터를 캐싱하는 서비스 노드로 해당 데이터를 제공하므로 동일 데이터를 반복적으로 검색할 필요가 없어집니다. 새로운 서비스 노드가 합류하여 스토리지 노드에서 가져온 데이터를 제공할 수 있습니다.

파일은 암호화 해시에 의해 시스템에서 검색됩니다. 이러한 해시는 파일이 시스템에 삽입되어 향후 사용을 위해 저장될 때 생성됩니다. 이 해시는 스토리지에 대한 유료 트랜잭션에 파일 주소를 연결하기 위한 식별자를 제공할 수 있으므로 블록 체인을 사용하여 파일을 저장하는 데 있어서 특히 중요합니다.

2.3 서비스 계층

Phantom은 스토리지 계층 서비스 위에서 동작하는 서비스 계층을 제공합니다. 이러한 서비스에는 HAProxy와 Jenga가 포함됩니다. 서비스 계층의 기본 기능은 Phantom을 "구세계" 인터넷 프로토콜 (예: DNS)에 연결하고 스토리지 계층에 대한 트래픽 관리를 제공하는 것입니다.

2.3.1 HAProxy

Phantom에는 HAProxy가 포함되어 있는데, 이 서비스는 IPFS 및 관련 클러스터의 API 종단점에 대한 개별 주소 지정 및 트래픽 처리를 제공합니다. 백엔드 트래픽 처리 외에, 시스템에 대한 프런트엔드 요청도 처리합니다. 이 서비스는 SSL을 활용하여 클라이언트와 서버 사이에 암호화된 통신을 제공합니다. 또한, 모든 수신 요청을 처리하여 데몬이나 클러스터로 전달되도록 합니다. HAProxy가 보호 수단으로 작동하므로 대상 애플리케이션에서 화이트리스트에 포함된 호출만 실행합니다. 모든 금지된 요청이 거부됩니다.

2.3.2 Jenga

아직까지는 IPFS를 기본적으로 지원하는 주류 브라우저가 없으므로 수신 요청을 특정 서버로 맵핑하는 방법이 필요합니다. 이 문제는 Chrome이나 Firefox 브라우저 확장 기능을 사용하여 브라우저에서 콘텐츠를 제공할 IPFS 노드를 선택함으로써 해결할 수 있지만 이상적인 방법은 아닙니다. Phantom에서 호스팅하는 웹사이트를 방문하기 전에는 최종 사용자가 제3자 소프트웨어를 설치하지 않아야 하기 때문입니다.

또 한 가지 해결책은 내부 로드 밸런서를 사용하는 것인데, 이 방법도 문제가 있습니다. 일차적 문제는 그것이 중앙집중식이라는 점입니다. 로드 밸런서가 실패하면 Phantom에 대한 모든 요청이 실패할 것입니다. 두 번째 문제는 시스템이 더 많은 트래픽을 처리할 수 있도록 확장되어야 하는 경우와 같은 처리량 또는 성능 문제에서 발견됩니다. 이 시스템은 세계적 수준의 파일 스토리지 시스템에서 실현 불가능한 전체 Phantom 네트워크의 처리량을 지원해야 합니다.

Jenga는 콘텐츠를 보는 최종 사용자가 추가 소프트웨어를 설치하지 않아도 작동하는 확장 가능한 솔루션을 제공함으로써 이러한 문제를 둘 다 해결합니다.

Jenga는 변경 사항이 있는지 최상위 DNS 항목을 관찰하고 변경 사항을 기록하는 DNS 모니터링 솔루션입니다. Jenga는 IPFS 클러스터와 관련된 변경 사항이 감지되면 클러스터의 모든 스토리지 노드를 업데이트합니다. Jenga는 모든 노드와의 지속적인 통신 상태를 유지함으로써 정상 DNS 상태에 대한 합의를 이끌어내고 이후에 비준수 노드를 시스템에서 퇴출시킬 수 있습니다. 이렇게 함으로써 공격자가 클러스터에 조인하여 잘못된 DNS 항목을 삽입하는 것을 방지하여 DDoS(Distributed Denial-of-Service: 분산형 서비스 거부) 공격 벡터를 시스템에서 제거합니다.

Jenga는 분산형 웹과 기존 인터넷(전적으로 DNS 레코드에만 의존) 사이에서 교량 역할을 합니다. Jenga는 동적 웹 주소 지정 시스템을 생성하고 시스템에 있는 레코드에 기초하여 한 노드에서 수천 개 노드로 트래픽을 쉽게 확장할 수 있도록 지원합니다. 이 기능은 최종 사용자에게 투명하게 작동하므로 시스템 작동을 위해 외부적인 상호 작용은 필요하지 않습니다. 기본적인 수준에서 Jenga는 시스템이 일부 중앙 서비스 중단 지점을 처리 할 수 있게 합니다. 즉, DNS 검열과 트래픽 성형 문제를 해결해 줍니다.

Jenga가 기능하려면 Jenga가 IPFS 클러스터의 연결된 모든 피어와 연결 상태를 유지해야 합니다. Jenga는 클러스터에서 변경 사항을 감지할 경우 DNS를 새 정보로 업데이트합니다. 노드가 오작동하거나 오프라인 상태인 경우 Jenga는 이에 대한 조치를 취하고 해당 피어의 할당된 CNAME 레코드를 제거하여 해당 피어를 제거합니다. 피어는 오류를 해결하고 나서 정상 상태를 Jenga에 보고한 후 시스템에 다시 조인할 수 있습니다.

외부 요인에 의해 게이트웨이가 호출될 때 클러스터의 피어 중 하나가 데이터를 호출자에게 제공하는 역할을 담당할 피어로 선정됩니다. 이 프로세스는 클러스터 전체에서 데이터 복제를 통해 완벽하게 수행됩니다.

새 사이트가 시스템에 조인하려면 사업자는 해당 게이트웨이를 가리키는 도메인에 대한 CNAME 레코드를 제공해야 합니다. 운영자가 해당 게이트웨이 사용을 원치 않을 경우 사업자는 고유한 게이트웨이를 가리키는 DNS 레코드를 생성할 수 있습니다. 클러스터는 여전히 데이터를 전달하겠지만 이 사이트는 서비스를 제공할 수 있는 모든 정상 노드 이용을 주로 보장하는 Phantom 게이트웨이의 이점을 잃게 됩니다.

3 보안 블록체인

콘텐츠 보안은 분산형 시스템에서 가장 중요한 부분입니다. 들어오는 데이터는 모두 손상되지 않은 상태로 나가야 하며 고객은 데이터의 정확성 여부를 신뢰해야 합니다. 블록체인 기술은 허위 입증 불가능한 원장을 통해 여러 신뢰 관련 문제를 해결하므로 Phantom에서 시스템 내 불변성과 진실성을 유지하는데 활용됩니다.

3.1 위임된 지분 증명

Shift는 위임된 지분 증명(Delegated Proof-of-Stake)을 통해 보안이 유지되는 분산형 블록체인으로 설명됩니다. 선정된 101(현재 숫자 N은 101임) 대리자가 시스템의 관리자로 활동합니다. 이들 대리자는 27초(블록 시간)마다 할당된 슬롯에 블록을 생성하고 Shift의 웹 호스팅 플랫폼에 대한 최종 트랜잭션을 원장에 제공합니다. 관리자는 계좌 잔고와 등록 상태를 추적할 뿐만 아니라, 개인 키와 공용 키 사이의 암호화 연결 시스템을 제공합니다.

시스템의 최종 사용자는 자신이 임의대로 사용할 수 있는 하나 이상의 개인 키를 가질 수 있으며 이러한 키를 사용하여 해당 시스템 내에서 토큰을 소유할 수 있습니다. 이 점은 Phantom을 호스팅할 블록체인과 결합될 때 특히 중요합니다. 사용자는 Shift 블록체인에서 Phantom 사이드체인으로 일부 토큰을 보내야 합니다.

3.2 Phantom 사이드체인

사이드체인은 상위 블록체인과 공존하는 블록체인입니다. 이 경우, Phantom에는 Shift 메인체인에 고정된 사이드체인이 있는데, 이 사이드체인은 Phantom용 토큰화된 백본을 제공합니다.

Phantom용 사이드체인 안에는 최종 사용자 토큰 잔액을 추적하는 별도의 원장이 있습니다. 이러한 토큰은 사용자에게 IPFS 클러스터 내에서 콘텐츠를 고정/고정해제하고 토큰을 교환하여 파일을 장기간 저장할 수 있는 기능을 제공합니다. 이 시스템을 지원하기 위해 최종 사용자는 노드 운영자로서 시스템에 조인하고 스토리지를 필요로 하는 사용자에게 초과 공간을 임대할 수 있습니다.

3.2.1 트랜잭션 타입

Shift에서 제공하는 기존 시스템을 기반으로 하는 사이드체인은 이 플랫폼에 국한된 새로운 기능을 구현합니다. 이 기능은 Shift 내에서 발견되는 트랜잭션 타입의 개념을 확장하므로, 사이드체인 내에서 사용할 수 있는 새로운 그룹의 트랜잭션 타입들이 생성될 것입니다.

타입 10 – 스토리지 요청
최종 사용자나 시스템은 클러스터 내에 콘텐츠를 저장해야 합니다. 이렇게 하기 위해 사용자는 요청을 클러스터 내 보안 스토리지에 제출합니다. 사이드체인에서 수신되고 블록체인으로 확인되면, 시스템 내에서 사용자를 위한 스토리지가 할당됩니다. 이 스토리지를 이용하여 사용자는 시스템에 파일을 추가할 수 있습니다.

타입 11 – 스토리지 반환
어느 시점에는 사용자가 스토리지를 더 이상 사용할 필요가 없을 수도 있습니다. 이 경우 사용자는 이 유형의 요청을 제출하여 토큰을 해제합니다. 트랜잭션이 확인된 후에는 시스템으로부터 사용자에게 토큰이 반환됩니다.

타입 12 – 스토리지 제공
시스템이 올바르게 작동하려면 시스템에 스토리지를 제공해야 합니다. 과다 스토리지가 있는 사용자는 요청(추가할 스토리지 양 포함)을 제출하여 네트워크에 스토리지를 제공할 수 있으며 이 경우 요청을 뒷받침하는 지분 증명(Proof-of-Stake)이 있어야 합니다.

타입 13 – 스토리지 회수

타입 11에서처럼 사용자는 토큰을 반환하고 네트워크에 스토리지를 제공하는 일을 그만두고자 할 수도 있습니다. 이 요청이 네트워크에 제출되고 확인되면, 스토리지 위탁과 관련된 고정 토큰이 사용자에게 반환됩니다.

3.3 외부 상호작용 – 배치

Phantom은 Shift 메인체인 애플리케이션 인터페이스를 통해 배포됩니다. 운영자가 Phantom을 고유한 용도로 배포하려면 운영자는 Shift 메인체인의 사본을 실행해야 합니다. 또한, 운영자는 Phantom 인터페이스를 사용하여 고유한 파일을 업로드하거나, 새 콘텐츠를 추가하기 위해 제공된 API 세트를 사용해야 합니다. Phantom 자가 배포 시 최종 사용자가 반드시 시스템과 인터페이스할 필요는 없습니다.

4 표시 계층

여러 계층화된 애플리케이션과 마찬가지로, 최종 사용자는 최상위 계층이나 표시 계층과 상호 작용합니다. Phantom에서 표시 계층은 Hydra로 구성되며 스토리지 및 서비스 계층과 함께 작동합니다.

4.1 Hydra – 콘텐츠 관리 시스템

콘텐츠 관리 시스템이란 기술 지식 없이 문서 및 사이트 콘텐츠를 게시하는 데 사용되는 웹 애플리케이션입니다. 최종 사용자가 일반 텍스트를 제출하면 소프트웨어가 일관된 방식으로 레이아웃을 렌더링합니다. 동적 콘텐츠 및 정기 업데이트를 포함하는 웹 사이트는 CMS가 없으면 운영하기 어렵습니다. 일부 공통 서버 측 언어로 작성된 소프트웨어와의 작동 기능 부족이나 여러 데이터베이스에 대한 지원 부족 등 IPFS의 몇 가지 제한을 해결하기 위해 사용자 지정 CMS가 개발되었습니다.

Hydra라고 하는 맞춤 CMS는 IPFS를 기반으로 한 CMS로 작동하는 새로운 기술입니다. Hydra는 Phantom의 파일 관리자와 함께 작동하며 현재 콘텐츠 추가, 수정 및 제거 등 일반적인 작업을 처리할 수 있습니다. 기본 기능 세트는 대부분의 사용자 니즈를 충족하며 코드베이스가 오픈 소스이므로 개발자가 자신만의 요구에 맞춰 소프트웨어를 맞춤화하고 향상시킬 수 있습니다. Hydra는 최종 사용자로 확장 가능하도록 작성되었으며 코드베이스는 모듈식으로 설계되었습니다. 예를 들면 사이트 페이지와 블로그 게시물이 동일한 렌더링 엔진을 공유하지만 스키마가 서로 다를 수 있습니다. 새 모듈 작성은 구성 항목을 지정하여 Node.js를 통해 프로그래밍 방식으로 수행됩니다. 결과적으로 생성된 파일은 IPFS를 통해서만 제공할 수 있으며 모든 렌더링이 클라이언트 측에서 발생합니다.

프런트엔드 및 백엔드 구성 요소가 분리되어 있습니다. 따라서 개발자는 Vue, React 또는 Angular 같은 기본 프레임워크를 사용할 수 있습니다. 데이터 파일 및 모듈식 구조가 JSON 파일로 렌더링되므로 Wordpress API 같은 외부 시스템과 함께 사용할 수 있습니다.

4.2 Phantom UI – 파일 관리자

Phantom 사용자 인터페이스는 최종 사용자가 시스템에 의해 관리되는 콘텐츠를 보고 수정할 수 있도록 하는 지능형 파일 관리 인터페이스를 함께 제공합니다. 최종 사용자는 Shift 계정을 사용하여 콘텐츠를 추적합니다. 콘텐츠 제출 요청이 이 계정과 연결되며 특정 시스템을 통해 사용자에게 제공됩니다. 따라서 네트워크는 게시된 후 파일과 파일 변경 사항을 표시할 수 있습니다.

사용자는 일반적인 현대식 운영 체제와 동일한 방식으로 저장된 콘텐츠를 관리할 수 있습니다. 각 사용자가 수행하는 작업이 클러스터로 전파됩니다. 이 인터페이스는 고급 코드 편집자에게 일반적으로 사용되는 모든 파일 형식에 대한 구문 강조로 완벽성을 제공합니다.

IPFS는 각 데이터 파일에 대한 고유 해시를 생성하여 동일한 콘텐츠가 호스트 또는 업로드되는 것을 방지합니다. 제출 전에 중복 파일을 식별할 수 있으므로 이 기능은 업로드 프로세스를 간소화합니다. 또한, 시스템을 효율적으로 작동할 수 있게 해주며 최종 사용자 및 운영자의 대역폭 사용량을 똑같이 줄여줍니다.

Phantom UI에는 Shift에서 호스팅된 스토리지 클러스터를 이용하는 호스팅된 도메인 이름의 주소 지정을 제어할 DNS 마법사가 포함되어 있습니다. 이 마법사는 콘텐츠 제출자가 고유 시스템을 호스팅해야 하는 필요성으로 인해 발생되는 단일 서비스 중단 지점을 제거합니다. Phantom은 Jenga를 사용하여 요청한 도메인에 대한 콘텐츠를 제공할 정상 노드 목록을 작성합니다.

4.3 콘텐츠 검색

시스템 안에 저장된 데이터는 위치 수준이 아닌 콘텐츠 수준에서 수행됩니다. 이 새로운 접근 방식은 여러 가지 이점을 제공합니다. 기본 이점은 데이터 위치가 더 이상 중요하지 않으므로 여러 노드가 동일 정보를 표시할 수 있고 데이터가 변경될 때 새 해시가 생성된다는 점입니다. 이러한 이점의 결합으로 파일 시스템이 더욱 더 지능적인 형태가 되어 머클 해시(merkle hash)(루트)와 하위 폴더 또는 파일의

상대 경로를 생성합니다.

웹사이트의 주소는 URL로 지정되며 해시를 통해 콘텐츠를 가져옵니다. 변경 가능한 해시는 도메인 확인 시스템에서 사용됩니다. 변경 가능한 해시는 최종 사용자가 변경 불가능한 해시와 결합된 자신의 개인 키를 사용하여 업데이트할 수 있습니다. 이 기능 덕분에 도메인 레코드 업데이트 없이도 콘텐츠를 업데이트할 수 있습니다.

5 보안 계층

어떤 시스템에서든 보안이 가장 중요한 문제입니다. 분산형 시스템의 경우, 안정성을 확보하고 운영 신뢰성을 구축하기 위해서는 근본적으로 보안이 유지되어야 합니다.

5.1 Shift 클러스터 보안

Shift 클러스터는 Phantom 내에서 매우 중요한 역할을 담당합니다. 클러스터 안에는 호스트에 대한 여러 인증 메커니즘이 있습니다. 이러한 메커니즘이 클러스터를 공격과 이 문서에 설명되지 않은 다른 위협에 대해 보호된 상태로 유지합니다.

첫 번째 인증 계층은 블록체인 수준에서 수행됩니다. 사용자는 약정한 스토리지 용량을 등록하는 타입 12 트랜잭션을 전송하여 블록체인에 대한 등록 프로세스를 완료해야 합니다. 이 프로세스가 수행되고 나면 사용자는 Phantom에 클러스터 참여자로 등록하여 조인 프로세스를 완료할 수 있습니다.

두 번째 계층에서는 사용자가 블록체인에 등록하는 데 사용되는 개인 키와 스토리지 클러스터의 암호화된 조인 키를 사용하여 애플리케이션을 시작해야 합니다. 그러고 나면 애플리케이션은 관련 스토리지 약정에 대한 블록체인을 검색하고 유효성을 확인합니다. 이후에는 애플리케이션이 Phantom 등록 시 발급된 키를 해독하여 사용자가 클러스터에 조인할 수 있도록 합니다.

5.1.1 초과 가입 방지

초과 가입을 방지하기 위해 클러스터 및 블록체인 약정 스토리지 허용량이 시스템을 통해 면밀하게 모니터링됩니다. 스토리지 가용성이 낮은 경우 데이터를 클러스터에 추가하고자 하는 사용자가 클러스터를 사용하는 데 더 높은 수수료를 지불하게 되므로 조인하여 데이터를 제공할 때 인센티브가 더 많아집니다. 시간이 경과함에 따라 사용자의 지속적인 스토리지 요구와 사업자의 공급이 동등하게 평형을 유지해야 합니다.

사업자는 계약이 만료되기 전에 언제라도 갱신 또는 추가할 수 있도록 하면서, 설정된 기간 동안 스토리지를 제공합니다. 사업자가 약정 기간이 끝나기 전에 운영을 중단할 경우 지분을 잃게 됩니다. 따라서 시스템을 유지하려면 사업자가 높은 가동 시간을 유지해야 합니다. 블록체인마다 각 클러스터 사업자에 마련된 허용 오프라인 시간 수가 있습니다.

앞서 언급한 바와 같이 사업자는 잘못된 행동을 할 경우 처벌을 받게 됩니다. 사업자의 자금 손실은 억제력이 커서 잘못된 행동을 처리하기에 충분합니다. 네트워크에 초과 가입하거나 네트워크 플러딩을 초래하는 등 사용자도 잘못된 행동을 할 수 있습니다. 이러한 타입의 잘못된 행동은 지분 자금의 임시 동결로 이어질 수 있습니다.

악의적인 행위를 하는 사용자는 일정 기간 동안 시스템으로 전송할 수 있는 콘텐츠의 양을 제한하는 방법으로 처리됩니다. 사용자는 해당 기간의 임계값이 초과된 후 개시하는 데 더 높은 비용이 부과되기 전에 해당 기간 동안 설정된 개수의 트랜잭션을 만들 수 있습니다.

5.2 데이터 프라이버시

시스템에 입력되는 콘텐츠에 대한 보안은 시스템 자체에 대한 보안만큼이나 중요합니다. 사용자에게 스토리지 전송 전에 데이터를 암호화하는 옵션이 제공됩니다. 하지만 암호화된 콘텐츠는 잠금 해제 키를 사용해야만 읽을 수 있습니다. 그러므로 사용자는 콘텐츠를 암호화할 때 주의해야 하며 자신의 개인 키를 적절히 보호해야 합니다.

Phantom 내에서 사용자는 자신 이외의 특정 수신자를 염두에 두고 콘텐츠를 암호화할 수 있습니다. 공용 키 목록을 제공하여 단지 수신자의 개인 키만을 사용하여 해독할 수 있는 해독 키를 포함하는 암호화된 메시지를 생성하는 데 사용할 수 있습니다.

5.3 불법 콘텐츠

분산형 시스템에서 불법 콘텐츠는 항상 자신을 위한 틈을 형성합니다. Phantom의 경우 극심한 불법 콘텐츠의 호스팅이 허용되지 않습니다. 불법 콘텐츠를 시스템에 삽입하려는 사용자가 발견될 경우 지분을 잃을 수 있으며 콘텐츠가 제거될 수도 있습니다. 이 시스템은 고정 콘텐츠만 유지하며 고정되지 않은 콘텐츠는 신속히 삭제됩니다. 이 경우 사업자의 권한이 사용자보다 보호되어야 하므로 이러한 운영은 반드시 필요합니다.

6 결론

Phantom은 블록체인에 의해 지원되는 세계 최초의 분산형 스토리지 애플리케이션 중 하나입니다. Phantom은 사이드체인으로 사용되는 Shift 블록체인과 분산형 애플리케이션을 기반으로 하여 구현됩니다. Phantom은 IPFS과 클러스터링, Jenga와 Hydra를 활용함으로써, 웹 호스팅 및 콘텐츠 전달을 위해 검열로 보호되는 플랫폼을 제공합니다.

참고 문헌

Amazon. (2018). *Summary of the amazon s3 service disruption in the northern virginia (us-east-1) region.* Retrieved from `https://aws.amazon.com/message/41926/` (accessed January 31, 2018)

Benet, J. (2014). *Ipfs - content addressed, versioned, p2p file system.* Retrieved from `https://filecoin.io/filecoin.pdf` (accessed January 31, 2018)

Chen, C. (2017). Tired of dmca, riaa now seeks isp cooperation in catching and stopping copyright infringement. *Privacy News Online.* (https://www.privateinternetaccess.com/blog/2017/02/tired-dmca-riaa-now-seeks-isp-cooperation-catching-stopping-copyright-infringement/ (accessed January 31, 2018))

Eckersley, P. (2007). *Comcast is also jamming gnutella (and lotus notes?).* Retrieved from `https://www.eff.org/deeplinks/2007/10/comcast-also-jamming-gnutella-and-lotus-notes` (accessed January 31, 2018)

Martin, J. (2013). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *SAGE journals.* (http://journals.sagepub.com/doi/abs/10.1177/1748895813505234 (accessed January 31, 2018))

Raphael, J. (2009). Isps join riaa's fight against piracy: Is your isp one of them? *PCWorld.* (https://www.pcworld.com/article/161978/riaa.html (accessed January 31, 2018))

Search.usa.gov. (2018). *Seize domain names - immigration and customs enforcement (ice) search results.* Retrieved from `https://search.usa.gov/search?affiliate=ice.gov&query=seize+domain+names&commit=Search` (accessed January 31, 2018)

to Marlene H. Dortch, Z. K. A. (2008). *In the matter of formal complaint of free press and public knowledge against comcast corporation for secretly degrading peer-to-peer applications, file no. eb-08-ih-1518.* Retrieved from `https://ecfsapi.fcc.gov/file/6520169715.pdf` (accessed January 31, 2018)